

**REMARKS**

Claims 1-11 are pending. Claims 1-11 have been amended for clarification and to correct minor grammatical errors. For example, mixed recitations of “said” and “the” have all been changed to “the.” There are no issues of new matter.

The drawings stand objected to for being hand-drawn and of insufficient quality for publication. Submitted herewith are formal drawings to replace the objected-to drawings. Withdrawal of the objection is therefore requested.

Claims 1-7 stand rejected under 35 USC 112, 2<sup>nd</sup> paragraph, as being indefinite because the term “said first device” lacks antecedent basis. This term has been replaced with “the IP device.” Withdrawal of the rejection is therefore requested.

Claims 1-11 stand rejected under 35 USC 102(b) as being anticipated by Foulkes (WO 02/30082). Applicants traverse the rejection.

Claim 1 is directed to a system for supporting a website. The system comprises an IP device located on a public network and a second device located outside the public network. A connection between the second device and the IP device is initiated by the second device.

Applicants’ claimed invention addresses a problem with public websites, which makes them vulnerable to unauthorized access of sensitive information or private source data. Websites typically have a listening function and a responding function. The listening function maintains open communication with a public network and receives requests for information from devices having access to the public network. The responding function retrieves information in response to the requests and determines whether the requesting devices are authorized to receive that information. A hacker can potentially trick the responding function into accepting the hacker as an authorized requestor, thereby giving the hacker access to sensitive information or private source data on the website. See, e.g., the specification, ¶ [0009]. Applicants have solved this problem by separating the listening function and the responding function into separate devices, where the responding

function is located on a private network, such that any communication between the listening function and the responding function is solely initiated by the responding function over a single connection with the listening function. See, e.g., the specification, ¶ [0011].

In contrast, Foulkes discloses an IP client 30 that sends a request for information to a target server 70 via a security server 40. To secure the target server 70, the security server 40 receives the request from the IP client 30, authenticates the IP client 30, and upon authentication forwards the request to the target server 70. However, the security server 40 does not initiate connection with the IP client 30. Rather, the IP client 30 initiates connection with the security server 40. See, e.g., Foulkes, Figure 6, S30, where the IP client sends an IP request, and Figure 5, S10, where the security server receives the IP request. See also Foulkes, page 7, lines 5-15. If it were not the IP client that initiated connection with the security server, then the security server would not have received the IP request from the client. Indeed, Foulkes clearly describes the security server as providing public access, which means that any device on the network having a request can initiate connection with the security server. See, e.g., Foulkes, page 7, lines 1-2. Foulkes also fails to disclose that the target server 70 initiates connection with the IP client 30. Indeed, Foulkes discloses that there is no direct connection between the target server 70 and the IP client 30. See, e.g., Foulkes, page 3, lines 7-15.

Whereas, in the system of Applicants' claim 1, it is the second device that initiates connection with the IP device, where the second device is the device having a responder application to process requests for information received from a listening function and the IP device is the device having the listening application to send the requests for information to the responder application. The device sending the requests cannot initiate connection with the device processing the requests. It is the other way around.

The Office Action asserts that "initialization starts when IP security server 40 acknowledges IP client request." See Office Action, page 7, lines 2-3. However, this assertion does not address

what the claims recite. The claims do not recite that connection is “initialized,” but that connection is “initiated.” The two words “initialized” and “initiated” have different meanings. As such, the assertion is not relevant to Applicants’ claims.

Therefore, since Foulkes fails to disclose a connection that is initiated by a second device outside of a public network with an IP device on the public network, claim 1 is not anticipated by Foulkes. Claims 2-7 also are not anticipated by Foulkes at least by virtue of their dependency from claim 1.

The same reasoning can be applied to claim 8, which recites similar distinguishing features. Moreover, claim 8 recites that the second device has a responder function. However, Foulkes does not disclose that either the IP client 30 or the security server 40 has a responder application, as described in the specification, ¶ [0009], for example. Therefore, claim 8 is not anticipated by Foulkes.

Claim 9 is directed to a method for increasing security for sensitive information or source data. The method includes, *inter alia*, providing an application that corresponds to a listening function of a website and providing an application that corresponds to a responder function of a website. The responder application initiates a communication channel to the listening application as a communication client.

In contrast, Foulkes discloses an IP client 30 having a web browser 31 that requests data from a target server 70 via a security server 40. The IP client 30 includes an IP application 32 that monitors and modifies the flow of IP traffic between the web browser 31 and the IP network. Thus, the web browser’s request is passed by the IP application 32 to the security server 40. See, e.g., Foulkes, page 9, lines 8-22. As described previously, the security server 40 receives the request from the IP client 30, authenticates the IP client 30, and upon authentication forwards the request to the target server 70. However, the security server 40 does not initiate a communication channel with the IP client 30. Nor does the target server 70, which has the information requested by the IP

client 30, initiate a communication channel with the IP client 30. Rather, it is the IP client 30 that initiates communication by sending the web browser request.

Moreover, Foulkes does not disclose that either the IP client 30 or the security server 40 includes a responder application, as described in the specification, ¶ [0009], for example.

Therefore, since Foulkes fails to disclose a responder application initiating a communication channel to a listening application as a communication client, claim 9 is not anticipated by Foulkes.

The same reasoning can be applied to claims 10 and 11, which recite similar distinguishing features. Therefore, claims 10 and 11 are not anticipated by Foulkes.

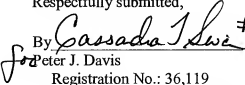
Withdrawal of the rejection is therefore requested.

In view of the above, each of the presently pending claims in this application is believed to be in immediate condition for allowance. Accordingly, the Examiner is respectfully requested to pass this application to issue. If it is determined that a telephone conference would expedite the prosecution of this application, the Examiner is invited to telephone the undersigned at the number given below.

In the event the U.S. Patent and Trademark Office determines that an extension and/or other relief is required, Applicants petition for any required relief including extensions of time and authorize the Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to **Deposit Account No. 03-1952** referencing docket no. **496332000300**.

Dated: November 1, 2007

Respectfully submitted,

By  #48,361  
for Peter J. Davis  
Registration No.: 36,119  
MORRISON & FOERSTER LLP  
1650 Tysons Blvd, Suite 400  
McLean, Virginia 22102  
(703) 760-7748